Accellion Share Securely™

AN ACCELLION WHITE PAPER

Secure File Sharing and Collaboration in the Cloud: Maximizing the Benefits While Minimizing the Risks

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

WP-SCC0911

Executive Summary

Cloud computing enables enterprises to meet their business IT requirements more nimbly and effectively than ever before. The opportunity to offer enterprise business applications from a private cloud, public cloud, or hybrid cloud configuration gives enterprises tremendous flexibility for maximizing the cost-effectiveness of IT deployments.

At the same time, the availability of free cloud-based services has created new security vulnerabilities for enterprise organizations. Employees are increasingly taking advantage of these free cloud services to share confidential information and collaborate with people outside the organization without adequate security, tracking, or visibility for the organization. Use of unmanaged cloud-based services puts organizations at risk for a data breach or non-compliance.

This white paper explores the considerations for deploying secure file sharing and collaboration in the cloud. It also discusses the security implications and requirements for ensuring protection of confidential information and compliance with industry and government regulations.

To learn more about the general requirements for secure collaboration, see our white paper, Security Essentials for Enterprise Collaboration.

Introduction

Cloud computing is transforming enterprise IT. In every area of operations, enterprises are increasingly choosing cloud services when they launch new services or replace traditional on-premise applications.

Evidence of this transformation is everywhere. The Software-as-a-Service (SaaS) market, which offers cloud-based applications over the Web, is growing six times faster than the rest of the software market, and it's expected to continue growing at 26% Compound Annual Growth Rate through 2014.[1] About 60% of enterprises are now using SaaS, up from 47% a year ago. Over the next five years, companies will spend over $112 billion on SaaS, Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS) combined, and world cloud services revenue will reach a whopping $148 billion.

Impressive as these numbers are, they probably under report the adoption of cloud services. Many cloud-based services are offered free of charge or for a small monthly fee. Departments and individual users subscribe to them through "quick-and-dirty" purchases outside the purview of the IT department, the finance department, and compliance officers. Since 40% of enterprises have no way of monitoring cloud services at all,[2] it's not surprising that a significant portion of cloud service usage goes undetected and unmonitored. Ignoring this adoption is risky, though, because these services are increasingly being used to transmit and store confidential data without adequate security safeguards, putting enterprises at risk for security breaches and compliance violations.

The Risks and Benefits of Collaboration in the Cloud

Nowhere are the both the benefits and the risks of cloud computing more evident than in the area of enterprise-class collaboration and file sharing.

Collaboration in the enterprise requires a scalable, secure, easy-to-use application where information can be readily discovered, shared, discussed, logged, and managed. Along with the need for anytime, anywhere access to information enterprise collaboration is well suited to leveraging the cost-effectiveness and elastic nature of cloud based services. With knowledge workers spending far too much time—between 15 to 30% of their time, according to IDC[3]—just looking for the information they need, enterprise collaboration offers opportunities for dramatic productivity gains. By posting files in a shared workspace, where information can be tagged, searched, versioned, and commented on, employees can collaborate effectively and productively with minimal time lost searching for information. They can create and evaluate information, instead of hunting for it.

However, the need for protecting intellectual property and ensuring compliance makes collaboration in the cloud a developing security nightmare for many

[1] http://www.cloudave.com/6785/idc-prediction-saas-revenue-growth-6x-faster-than-all-software/
[2] http://ubmtechnology.mediaroom.com/index.php?s=43&item=3030
[3] Spinuzzi, Hart-Davidson, and Zachry, "Modeling Knowledge Work," http://www.drc.utexas.edu/main/sites/default/files/040505-1.pdf

Public Cloud Services in Action: Clyde & Co. LLP

On April 14, 2010 the EyjafjallajÖkull volcano in Iceland erupted, sending plumes of smoke into the air and shutting down nearly all air transportation in Europe. Clyde & Co. LLP, an international law firm based in London, faced business disruptions when the courier company they relied on to share urgent legal documents was grounded.

Leveraging the Accellion Secure File Transfer Hosted Cloud Service, the firm was able to resume sharing confidential files with clients and partners within minutes. Because the Accellion Hosted Cloud Service was hosted by Accellion, rather than by Clyde & Co.'s own data center, the service was made available immediately.

- *Cloud Architecture: Public SaaS*
- *Benefit: Immediate provisioning of secure file transfer services*
- *Risk Averted: Lost revenue and business disruption from a natural disaster*
- *Security: Protects confidential client data in transit and at rest*

enterprise organizations.

The ready availability and accessibility of inexpensive cloud-based collaboration solutions has resulted in business users bringing solutions into the workplace that do not provide the tracking and reporting necessary for compliance.

Lacking a secure, convenient solution from IT departments for sharing files and collaborating, users are flocking to dropbox-type SaaS services.[4] Using an inexpensive, free cloud service for sharing files, employees get their work done, even if they violate internal policies and industry regulations. A Web browser, a credit card, and a click-through SaaS subscription form can instantly undermine hundreds of thousands of dollars of investments in firewalls and data loss prevention technologies—but most employees are oblivious to the security risks.

Collaboration in the Cloud: Private, Public, and Hybrid

The selection of enterprise collaboration solutions in the enterprise has mostly been driven by business user features with little discussion on the benefits and security considerations. How should enterprises go about selecting the best architecture for their collaboration needs? Should they implement a collaboration solution on-premise, in the cloud, or in a hybrid configuration that combines both models? What factors should enterprises consider to ensure that their implementation of a collaboration solution doesn't jeopardize the security and compliance they're working so hard to achieve?

Enterprises have three main choices: private clouds, public clouds, and hybrid clouds.

Public Cloud

A public cloud is shared by all members of the public who subscribe to the service. There are three types of public cloud services: IaaS, PaaS, and SaaS.

IaaS

A public-cloud Infrastructure-as-a-Service (IaaS) offering lets users access a variable number of instances of IT infrastructure, such as Linux servers or VMware instances. Anyone can sign up for an IaaS offering. IaaS resources can be used for any length of time—from a few minutes to a few years—depending on how long a customer requires them. Two of the most popular IaaS services are Amazon EC2 and Rackspace. Many popular SaaS applications (described below) run on Amazon EC2, rather than on the application provider's own infrastructure.

PaaS

A Platform-as-a-Service (PaaS) offering provides variable instances of an application environment such as the LAMP stack (an application environment featuring a Linux operating system, an Apache Web server, a MySQL database, and the Python programming language).

[4] For example, YouSendIt recently announced that its sales grew 1,415% over three years—a clear sign of growing adoption, with or without the blessing of enterprise IT departments. http://www.yousendit.com/aboutus/press/2010-inc500-fastest-growing

Private Cloud Services in Action: GSD&M Idea City

GSD&M Idea City, part of the Omnicom Group, is an advertising agency known for growing clients' businesses and contributing to communities around the world.

As a creative agency, GSD&M Idea City works with media files that can grow well beyond the normal file-size limits of email. Keeping client files about upcoming launches secure and being in compliance with local data storage requirements is not a flashy way to delight their customers, but without it, the great work they do could be overshadowed by possible security and compliance complications. In this case, Idea City chose Accellion in part because it's flexible enough to work easily in Idea City's private cloud environment, where it facilitates the secure collaboration the company considers vital to its success.

Support for virtualized environments was a key requirement. Dallas Larose, enterprise systems supervisor, explains: "We currently run more than 60% of our systems in a VMware virtual server farm. Ideally, we'd like all new application purchases to work in this virtual environment."

- *Architecture: Private Cloud*
- *Benefit: Improved collaboration while leveraging VMware virtual server farm*
- *Risk Averted: Lost productivity and business agility because of cumbersome file-sharing practices*
- *Security: Protects confidential design files in transit and at rest*

SaaS

Software-as-a-Service (SaaS) offerings make applications available to individual subscribers or groups of subscribers over the Internet. Businesses can sign up for the applications and access them immediately. There's no need to invest in capital equipment and equipment maintenance; application provisioning becomes simply an operational expense. SaaS offerings include "freemium" applications that are free to individual users or free with a limited number of features, but not free when more users or features are added.

Data Security and Compliance Risks for Public Clouds

Most public cloud offerings pose some kind of security or compliance risk for the enterprise.

An IaaS or PaaS offering might be designed to prevent one customer from seeing another customer's data, but there's no guarantee that a public cloud subscriber will have exclusive access to resources such servers. On the contrary, users should assume they won't have exclusive access to these resources. A clever or determined hacker might be able to exploit this vulnerability. A careless administrator might leave confidential data vulnerable to unauthorized access or tampering.

Employees often use free cloud-based SaaS applications as a low-cost, convenient way of getting things done, but SaaS applications create data security risks if they transmit or store confidential data outside the control or oversight of the IT department and compliance officers. Also, if different departments in an organization do not coordinate their SaaS subscriptions, they might end up adopting incompatible applications. These incompatibilities might increase the difficulty of monitoring and securing data services.

Private Cloud

Most often, private clouds are run and managed in a private data center owned by the enterprise. Gartner, however, considers cloud services private if they run even at a third-party hosting site, so long as only a single enterprise has access to services and their infrastructure. Enterprises are deploying private clouds to take advantage of the convenience and elasticity of cloud computing, while keeping control of data and IT resources.

Data Security and Compliance Risks for Private Clouds

Assuming the third-party data center is secure, the data in a private cloud should be as secure as data in a private data center owned by the enterprise.

Hybrid Cloud

A hybrid solution combines private and public services. Hybrid cloud configurations are often used to expand computing and storage capacity to accommodate spikes in demand. For example, an enterprise might normally run an application on a private cloud in its own data center, but when demand increases, the enterprise might launch additional application instances in a public cloud. The enterprise pays only for the public cloud services it uses, so as soon as demand drops, the additional application instances are released. This hybrid model quickly becomes much more cost-effective than purchasing additional server capacity on-premise and having that capacity sit idle when application usage is below peak levels.

Hybrid Cloud Services in Action: Large Consumer Brand

A large retail alcohol and spirits producer needed to help its digital media and marketing teams share information more easily with outside agencies, while also streamlining approval processes. Artwork for ad campaigns can easily consume tens or hundreds of megabytes. Deploying a secure file transfer solution that complemented email without overwhelming seemed like the thing to do.

The company deployed an Accellion physical appliance in one of its European offices. The on-premise deployment enables the global marketing teams to take advantage of their well-designed, ultra-speedy internal network.

The company also deployed Accellion services in the cloud to offer similar advantages and flexibility to marketing staff globally. As a result, the company has cloud-based appliances in America, Asia and Europe to extend the range of its Accellion secure file transfer services.

- Architecture: Hybrid Cloud
- Benefits: Global reach to organization and clients and streamlined approval processes
- Risk Averted: Lost productivity and business agility because of cumbersome file-sharing practices and time-consuming approval processes
- Security: Leveraged existing security infrastructure at main office and protects confidential data in transit and at rest

Data Security and Compliance Risks for Hybrid Clouds

The public cloud portion of a hybrid solution is prone to all the security risks commonly associated with public clouds. These risks aren't insurmountable, but enterprises must be sure to address them.

Enterprises with a global collaboration solution might need to deploy a hybrid cloud for compliance with data privacy regulations. In European countries, for example, regulations mandate that customer data be stored within the country where the customers live. A local private cloud in Europe might need to work alongside public cloud deployments in other countries.

Forecasting Cloud Architectures

Public cloud services such as Amazon EC2 and Rackspace are popular with organizations of all sizes. Nonetheless, Gartner expects that most enterprises will invest also in private cloud services for the next few years. Private clouds promise to provide more rigorous data security, which is essential for services involving confidential data such as customer records and financial statements. Private clouds might also strike many enterprises as more reliable, especially after the much publicized outage of Amazon EC2 in April 2011.

To balance data security and IT costs, hybrid cloud deployments will likely become the norm for enterprise deployments of portals, content, and collaboration as enterprise organizations balance security and cost management.[5] Gartner notes: "Most private-cloud-computing architectures should be designed with the future use of hybrid cloud computing in mind, providing more choices and a potential migration path to public cloud services as they mature, in an evolutionary way."

Cloud Architectures and Secure Collaboration

How should enterprise organizations pick the right cloud deployment option for their secure collaboration services?

By hosting collaboration services in a cloud, enterprises ensure that as workloads increase or special demands arise, users will always have access to the tools, data storage, and computing power they need. All cloud deployments—public, private, or hybrid—should be able to deliver the scalability and availability essential for business continuity, even during peak demand times.

The choice of private cloud or public cloud may end up being decided by an enterprise's assessment of the security requirements and industry regulations that apply to the data being processed or stored. Healthcare organizations, for example, might choose to only use private cloud services for any applications handling protected health information (PHI) because of the stringent data privacy regulations set forth in HIPAA, and because violating those regulations can lead to multi-million dollar penalties. For non-confidential data, public cloud services may be fine—and less expensive, as well.

[5] http://www.accellion.com/blog/2011/03/observations-from-gartner-portals-content-and-collaboration-summit-part-i/

The table below weighs the benefits of each cloud deployment option for enterprise collaboration.

Cloud Architecture for Secure Collaboration	Why to Use . . .	But Keep in Mind . . .
Public Cloud (SaaS offering)	• Easy-to-use • Inexpensive • Users can help themselves • Scalable	• Not monitored by IT • Possible channel for data leaks • Difficult to audit unless audit features have been specifically designed in • No assurance that it complies with industry regulations such as GLBA or HIPAA • Possible unscheduled downtime
Public Cloud (IaaS offering) Example: Amazon EC2	• Inexpensive • Scalable • Can be monitored by IT	• Multi-tenant configurations might put private data at risk, unless the solution has been designed to comply with rigorous security standards such as FIPS 140-2 • Need for disk encryption • Possible unscheduled downtime
Private	• Scalable resources managed in house • Secure	• Requires in-house management • Might not scale as quickly as public solutions
Hybrid	• Offers the most control and security, while enabling business users and others to take advantage of greater scalability when needed	• Requires enterprises to carefully monitor cloud usage to ensure that sensitive data (e.g., PHI protected by HIPAA) is never posted on a public cloud and always tracked by the enterprise

By carefully assessing the security requirements, accessibility requirements, and budget of a collaboration service, enterprises can select the optimum cloud deployment scenario for delivering that service to its user community.

Accellion Secure Collaboration

Accellion provides enterprise-class secure collaboration and managed file transfer solutions that enable users to collaborate with their colleagues, clients, and partners, while adhering to security and compliance best practices. Users of the Accellion solution can quickly, easily, and securely share files from anywhere, at any time and on virtually any device, including mobile devices. The solution provides fine-grained access controls, integrates with enterprise LDAP and Active Directory services, provides built-in Anti-Virus protection, and gives administrators and compliance officers the logging and management features they need to comply with company security policies and industry regulations.

Support for Cloud Deployment Options

Accellion offers the choice of contracting cloud-hosting services directly through Amazon, a VMware vCloud hosting provider, or using an Accellion-in-the-Cloud service, in which case Accellion manages the installation and ongoing maintenance of the Accellion-in-the-Cloud service for the customer.

Customers can also choose to deploy Accellion virtual appliances themselves in any of following virtual environments:

- Public cloud:
  - VMware vCloud
  - Amazon EC2
- Private cloud or on premise:
  - VMware
  - Citrix XenServer
  - Microsoft Hyper-V
  - Accellion physical appliance
- Hybrid cloud:
  - Any combination of the above (for example, Citrix XenServer in a private cloud that is integrated with Accellion-in-the-Cloud instances running on Amazon EC2)

> "*Accellion's cloud solution leverages the latest in file sharing protocols and shared server hosting platforms which means I don't have to worry about server crashes or overloading the network. Stability and dependability are a given with this solution. As a result, we are able to focus our efforts on creating great applications for our customers, not spending time and money delivering them.*"
>
> –James Tuttle, IT Director
> TCS Healthcare Technologies

Customers can mix deployment options however they like. Should a sudden spike in workloads require an enterprise to increase the capacity of its workspaces, the IT department can launch additional Accellion virtual appliances in a private or public cloud, augmenting whatever physical or virtual appliances were running previously. Lines of business have the freedom to choose the public, private, or hybrid deployment option that best supports their business and IT goals of the moment.

All hosted, cloud, virtual, and on-premise Accellion solutions have been FIPS 140-2 certified, so customers can be confident that their file sharing and

collaboration workspaces meet the data security standards of U.S. governmental agencies.

Conclusion

Cloud computing enables enterprises to meet their business IT requirements more nimbly and effectively than ever before. For essential IT services like secure collaboration, the opportunity to run services in a private cloud, public cloud, or hybrid configuration offers enterprises important flexibility for maximizing the security and cost-effectiveness of their deployments.

The Accellion Secure Collaboration offers enterprises a proven solution for working with all three cloud deployment models. Built-in support for popular environments such as VMware, Citrix XenServer, Microsoft HyperV, and Amazon EC2 gives enterprises the broadest possible flexibility for managing secure collaboration services in the cloud. Enterprises can adopt the Accellion solution to give users the feature-rich, easy-to-use collaboration services they need today, while ensuring they have the flexibility to meet the demands of their evolving cloud strategy tomorrow.

For more information, please visit www.accellion.com.

www.accellion.com **info@accellion.com**